

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Peter Nesz, <i>et al.</i>	§	Group Art Unit:	2446
Application No	10/531,753	§	Examiner:	Taha, Shaq
Filed:	09/20/2005	§	Confirmation No:	6062
Attorney Docket No:	P17299-US1	§		
Customer No.:	27045	§		

For: Method and Arrangement for Preventing Illegitimate Use of IP Addresses

Via EFS-Web

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313.1450

CERTIFICATE OF TRANSMISSION BY EFS-WEB

Date of Transmission: February 7, 2011

I hereby certify that this paper or fee is being transmitted to the United States Patent and Trademark Office electronically via EFS-Web.

Type or Print Name: Jennifer Hardin

/Jennifer Hardin/

APPEAL BRIEF SUBMITTED UNDER 35 U.S.C. §134

This Appeal Brief is submitted to appeal the rejection of claims 13-22, which are all of the pending claims in this application, as presented by the Primary Examiner in a Non-Final Office Action dated September 10, 2010. Whereas fees for a Notice of Appeal and Appeal Brief were paid for previously-filed appeals, **which the Examiner did not answer**, no new fees are due.

Real Party in Interest

The real party in interest, by assignment, is: Telefonaktiebolaget LM Ericsson (publ)
SE-164 83
Stockholm, Sweden

Related Appeals and Interferences

A prior Appeal was filed on September 30, 2009, to appeal the decisions of the Primary Examiner set forth in a Final Office Action dated March 31, 2009, finally

APPLICANTS' APPEAL BRIEF

rejecting claims 13-22. **Rather than answer that appeal**, the Examiner re-opened prosecution and issued a new basis of rejection in the Non-Final Office Action dated January 12, 2010. A second Appeal was filed on June 14, 2010, to appeal the decisions of the Primary Examiner set forth in that Office Action. **Rather than answer that appeal**, the Examiner re-opened prosecution and issued a new basis of rejection in the Non-Final Office Action dated September 10, 2010; the Applicants now appeal the new basis of rejection.

Status of Claims

Claims 1-12 were previously cancelled and are not appealed. Claims 13-22 remain pending, each of which are rejected and form the basis for this Appeal.

Status of Amendments

The claims set out in the Claims Appendix include all entered amendments. No amendment has been filed subsequent to the final rejection.

Summary of Claimed Subject Matter

Claim Elements	Specification Reference
13. A method for preventing illegitimate use of an Internet Protocol (IP) address by a subscriber device in an IP network, the network including a switch node and at least one DHCP server, said subscriber device in communication with the switch node, the method including the steps of:	Page 5, line 33, <i>et seq.</i>
creating a list of trusted ones of the DHCP servers in said switch node;	Page 6, line 3, <i>et seq.</i>
transmitting by the subscriber device a DHCP request message for an IP address;	Page 6, line 9, <i>et seq.</i>
receiving a reply message by said switch node which carries an assigned subscriber IP address;	Page 6, line 11, <i>et seq.</i>
analysing the reply message by said switch node to be a DHCP message and having a source address from one of the trusted DHCP servers;	Page 6, line 15, <i>et seq.</i>
updating a filter dynamically in the switch	Page 6, line 21, <i>et seq.</i>

node, the filter storing an identification of the subscriber device and the assigned subscriber IP address;	
transmitting a frame from the subscriber device using a source IP address;	Page 6, line 26, <i>et seq.</i>
comparing in the filter said source IP address with the stored subscriber IP address; and,	Page 6, line 27, <i>et seq.</i>
discarding said frame when said source IP address differs from the stored subscriber IP address.	Page 6, line 31, <i>et seq.</i>

Claim Elements	Specification Reference
18. A switch node in an Internet Protocol (IP) network adapted to prevent illegitimate use of an IP address by a subscriber device, the switch node including:	Page 5, line 5, <i>et seq.</i> Page 5, line 33, <i>et seq.</i>
at least one port for communication with a subscriber device;	Page 5, line 7, <i>et seq.</i>
an uplink port for communication with DHCP servers in the network; and,	Page 5, line 5
a filter device having a list of trusted ones of the DHCP servers, the filter device being associated with the ports; wherein the switch node is operative to:	Page 6, line 3, <i>et seq.</i>
receive a subscriber IP address request message from a subscriber device, analyse it to be a DHCP request message and transmit it on the uplink port;	Page 6, line 9, <i>et seq.</i>
receive a reply message on the uplink port, analyse it to be a DHCP reply message having a source IP address from one of the trusted DHCP servers on the list;	Page 6, line 11, <i>et seq.</i> Page 6, line 15, <i>et seq.</i>
dynamically update the filter with an identification of the subscriber device and a corresponding assigned subscriber IP address contained in the DHCP reply message;	Page 6, line 21, <i>et seq.</i>
receive a frame with a source IP address from a subscriber device;	Page 6, line 26, <i>et seq.</i>
compare in the filter said source IP address with the stored subscriber IP address for the subscriber device; and,	Page 6, line 27, <i>et seq.</i>
to discard said frame when said source IP address differs from the stored subscriber IP address.	Page 6, line 31, <i>et seq.</i>

The specification references listed above are provided solely to comply with the USPTO's current regulations regarding appeal briefs. The use of such references should not be interpreted to limit the scope of the claims to such references, nor to limit the scope of the claimed invention in any manner.

Grounds of Rejection to be Reviewed on Appeal

- 1.) Whether claims 13, 14, 16-20, 21 and 22 are anticipated, under 35 U.S.C. §102(b), by Lim, *et al.* (U.S. Patent No. 5,884,024); and,
- 2.) Whether claims 15 and 20 are unpatentable over Lim in view of Maufer, *et al.* (U.S. Patent Publication No. 2003/0233576).

Arguments

1.) CLAIMS 13, 14, 16-20, 21 AND 22 ARE NOT ANTICIPATED BY LIM, ET AL.

The Examiner has now rejected claims 13, 14, 16-19, 21 and 22 as being anticipated by Lim, *et al.* (U.S. Patent No. 5,884,024). The Applicants traverse the rejections.

It is first noted that the claims presently at issue were first presented in Applicant's response filed on January 23, 2009, to the Examiner's first non-final Office Action dated October 23, 2008, in which the Examiner rejected claims 13-16 and 18-21 as being obvious over Sitaraman, *et al.* (U.S. Patent No. 6,427,170) and Alkhatib, *et al.* (U.S. Patent Publication No. 2004/0044778), and claims 17 and 22 as unpatentable over Sitaraman, Alkhatib and Taylor, *et al.* (U.S. Patent Publication No. 2002/0065919). No subsequent amendments have been made to the claims. Subsequent to Applicant's response containing those claim amendments, the Examiner issued a Final Office Action on March 31, 2009; in that action, the Examiner rejected claims 13-16 and 18-21 as being obvious over Sitaraman, Alkhatib and Lim, *et al.* (U.S. Patent No. 5,884,024), and claims 17 and 22 as being unpatentable over Sitaraman, Alkhatib and Taylor¹. The Applicants then, in a Request for Reconsideration filed on June 1, 2009, presented

arguments as to why the teachings of Lim failed to cure the deficiencies in the teachings of Sitaraman and Alkhatib. The Examiner, however, maintained that basis of rejection in an Advisory Action dated June 30, 2009. The Applicants then filed their first appeal on September 30, 2009. Rather than answer that appeal, the Examiner re-opened prosecution and issued a new basis of rejection in a Non-Final Office Action dated January 12, 2010; that office action rejected claims 13-16 and 18-21 as being unpatentable over Massarani, *et al.* (U.S. Patent No. 6,393,484) and Larson, *et al.* (U.S. Patent Publication No. 2004/0107286), and claims 17 and 22 as unpatentable over Massarani, Larson and Taylor, *et al.* (U.S. Patent Publication No. 2002/0065919). The Applicant's immediately filed an appeal of that basis of rejection on June 14, 2010. Rather than answer that appeal, the Examiner *again* re-opened prosecution and issued a new basis of rejection in the Non-Final Office Action dated September 10, 2010; the Examiner's "new" basis of rejection is that claims 13, 14, 16-20, 21 and 22 are anticipated by Lim, et al. (U.S. Patent No. 5,884,024); *i.e.*, the Examiner now relies on Lim as an anticipatory reference, when it was first relied on as a secondary reference in the Final Office Action dated March 31, 2009. The Applicants now appeal the "new" basis of rejection.

It must be remembered that anticipation requires that the disclosure of a single piece of prior art reveals every element, or limitation, of a claimed invention. Furthermore, the limitations that must be met by an anticipatory reference are those set forth in each statement of function in a claims limitation, and such a limitation cannot be met by an element in a reference that performs a different function, even though it may be part of a device embodying the same general overall concept. Whereas Lim fails to teach each and every limitation of claims 13, 14, 16-20, 21 and 22, those claims are not anticipated thereby.

Claim 13 recites:

13. A method for preventing illegitimate use of an Internet Protocol (IP) address by a subscriber device in an IP network, the network including a switch node and at least one DHCP server, said

¹ Although not indicated by the Examiner, it was assumed that the rejection of claims 17 and 22 was also premised on the teachings of Lim, since those claims are dependent from claims 13 and 18, respectively.

subscriber device in communication with the switch node, the method including the steps of:

creating a list of trusted ones of the DHCP servers in said switch node;

transmitting by the subscriber device a DHCP request message for an IP address;

receiving a reply message by said switch node which carries an assigned subscriber IP address;

analysing the reply message by said switch node to be a DHCP message and having a source address from one of the trusted DHCP servers;

updating a filter dynamically in the switch node, the filter storing an identification of the subscriber device and the assigned subscriber IP address;

transmitting a frame from the subscriber device using a source IP address;

comparing in the filter said source IP address with the stored subscriber IP address; and,

discarding said frame when said source IP address differs from the stored subscriber IP address. (emphasis added)

The Applicants' invention is directed to preventing the illegitimate use of an Internet Protocol (IP) address by a subscriber device, commonly referred to as "spoofing." The novel method has the further advantage of preventing a device from obtaining an IP address from an illegitimate DHCP server. The novel method includes providing a filter in a switch node through which a subscriber device accesses the IP network. The switch node maintains a list of trusted DHCP servers which are conventionally used to assign an IP address to subscriber devices. When the switch node receives a DHCP request for an IP address from a subscriber device, the switch node examines the reply message that carries the assigned subscriber IP address and analyzes it to confirm it has a source address from one of the trusted DHCP servers. The switch node then dynamically updates the filter and stores an identification of the subscriber device and the assigned IP address. Subsequently, when the subscriber device transmits a frame, the switch node confirms in the filter that the source IP address of the frame matches the stored subscriber IP address and, if not, the switch node discards the frame. That combination of functions is not taught by Lim.

With respect to the claim limitation "creating a list of trusted ones of the DHCP servers in said switch node," the Examiner refers to column 2, lines 52-55. The

undersigned has reviewed that portion of Lim and can find no teaching of creating a list of trusted DHCP servers in a switch node. What Lim teaches is a "secure DHCP relay agent that forwards DHCP messages between the client systems and DHCP servers." There is no teaching therein, *however*, of such relay agent storing a list of trusted DHCP servers. The use of the list of trusted DHCP servers is important with respect to the subsequent claim limitations, wherein a reply message [from a DHCP server] is received and analysed to determine whether it has a source address from one of the trusted DHCP servers.

With respect to the claim limitation "analysing the reply message [by said switch node] to be a DHCP message and having a source address from one of the trusted DHCP servers," the Examiner states that:

"the secure IP relay agent 'learns' the IP addresses *that are assigned to each client system* 102, wherein the relay agent that is included on the switch analyzes the DHCP messages *sent from client to DHCP server and vice-versa* [sic], (Lim et al., Col. 5, lines 50-55)"

The "reply message" in the subject claim limitation is from the DHCP server, not from the client system. Lim does teach a "secure IP relay agent that 'learns' the IP addresses that are assigned to each client system," but it does not each storing a list of trusted DHCP servers *and* analyzing a reply message from a DHCP server to determine whether it has a source address from one of the trusted DHCP servers. In stating that Lim teaches "analyz[ing] the DHCP messages sent from client to DHCP server *and [vice versa]*," it is assumed that the Examiner is asserting that the secure IP relay agent taught by Lim also analyzes DHCP reply messages sent from a DHCP server. The undersigned has reviewed the teachings of Lim, *however*, and can find no such teaching. Although Lim does describe a "trusted identifier," that parameter is only included in DHCP broadcast messages sent from a client device to a DHCP server. It does not appear that there is any teaching in Lim to: 1) create a list of trusted ones of DHCP servers in a switch node; 2) receive a DHCP reply message, in response to a subscriber device transmitting a DHCP request message for an IP address; and, 3) analyze the reply message by the switch node to be a DHCP message *and having a source address from one of the trusted DHCP servers*. By checking whether a reply message has a source address from one of the trusted DHCP servers, the Applicants' invention goes beyond the teachings of the prior art to ensure that a device does not

obtain an IP address from an illegitimate DHCP server. Lim fails to teach that unique functionality. Therefore, the Examiner has not established a *prima facie* case of anticipation of claim 13. Whereas claim 18 contains limitations analogous to those of claim 13, it is also not anticipated by Lim. Furthermore, whereas claims 14, 16 and 17 are dependent from claim 13 and claims 19, 21 and 22 are dependent from claim 18, and include the limitations of their respective base claim, those claims are also not anticipated by Lim.

2.) CLAIMS 15 AND 20 ARE PATENTABLE OVER LIM AND MAUFER

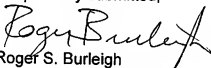
The Examiner rejected claims 15 and 20 as being unpatentable over Lim, *et al.* (U.S. Patent No. 5,884,024) in view of Maufer, *et al.* (U.S. Patent Publication No. 2003/0233576). As established *supra*, Lim fails to anticipate independent claims 13 and 18. The Examiner has not pointed to any teaching in Maufer that would overcome the deficiencies in the teachings of Lim and, thus, claims 13 and 18 are not obvious in view of a combination of Lim and Maufer. Therefore, whereas claims 15 and 20 are dependent from claims 13 and 18, respectively, and include the limitations thereof, they are also not obvious over Lim and Maufer.

* * *

CONCLUSION

The claims currently pending in the application are patentable over the cited prior art, and the Applicants request that the Examiner's rejections be reversed and the application be remanded for further prosecution.

Respectfully submitted,



Roger S. Burleigh
Registration No. 40,542
Ericsson Patent Counsel

Date: February 7, 2011

Ericsson Inc.
6300 Legacy Drive, M/S EVR1 C-11
Plano, Texas 75024

(972) 583-5799
roger.burleigh@ericsson.com

CLAIMS APPENDIX

1-12. (Cancelled)

13. (Previously Presented) A method for preventing illegitimate use of an Internet Protocol (IP) address by a subscriber device in an IP network, the network including a switch node and at least one DHCP server, said subscriber device in communication with the switch node, the method including the steps of:

creating a list of trusted ones of the DHCP servers in said switch node;

transmitting by the subscriber device a DHCP request message for an IP address;

receiving a reply message by said switch node which carries an assigned subscriber IP address;

analysing the reply message by said switch node to be a DHCP message and having a source address from one of the trusted DHCP servers;

updating a filter dynamically in the switch node, the filter storing an identification of the subscriber device and the assigned subscriber IP address;

transmitting a frame from the subscriber device using a source IP address;

comparing in the filter said source IP address with the stored subscriber IP address; and,

discarding said frame when said source IP address differs from the stored subscriber IP address.

14. (Previously Presented) The method according to claim 13, further comprising the step of storing in the filter a subscriber MAC address, a subscriber physical port number, a subscriber virtual LAN identity and a lease time interval for the assigned subscriber IP address.

15. (Previously Presented) The method according to claim 13, wherein the subscriber IP address is statically assigned and handled by the DHCP servers.

16. (Previously Presented) The method according to claim 14, the method including deleting the subscriber identification and the corresponding assigned subscriber IP address from the filter when the lease time interval is out.

17. (Previously Presented) The method according to claim 13, the method further comprising the steps of:

- counting a number of attempts (n) from the subscriber to use an illegitimate IP address;

- comparing the number (n) of the attempts with a threshold number (N);

- sending a warning signal when the number of attempts exceeds a threshold criteria.

18. (Previously Presented) A switch node in an Internet Protocol (IP) network adapted to prevent illegitimate use of an IP address by a subscriber device, the switch node including:

- at least one port for communication with a subscriber device;

- an uplink port for communication with DHCP servers in the network; and,

- a filter device having a list of trusted ones of the DHCP servers, the filter device being associated with the ports; wherein the switch node is operative to:

- receive a subscriber IP address request message from a subscriber device, analyse it to be a DHCP request message and transmit it on the uplink port;

- receive a reply message on the uplink port, analyse it to be a DHCP reply message having a source IP address from one of the trusted DHCP servers on the list;

- dynamically update the filter with an identification of the subscriber device and a corresponding assigned subscriber IP address contained in the DHCP reply message;

- receive a frame with a source IP address from a subscriber device;

- compare in the filter said source IP address with the stored subscriber IP address for the subscriber device; and,

- to discard said frame when said source IP address differs from the stored subscriber IP address.

19. (Previously Presented) The switch node according to claim 18, wherein the switch node is further operative to store in the filter a subscriber MAC address, a subscriber physical port number, a subscriber virtual LAN identity and a lease time interval for the assigned subscriber IP address.

20. (Previously Presented) The switch node according to claim 18, wherein the subscriber IP address comprises a statically assigned address which is handled by the DHCP servers.

21. (Previously Presented) The switch node according to claim 19, wherein the switch node is further operative to delete the subscriber identification and the corresponding assigned subscriber IP address from the filter when the lease time interval expires.

22. (Previously Presented) The switch node according to claim 18, wherein the filter comprises a counter operative to count a number (n) of discarded frames on the subscriber port, to compare the number (n) of the discarded frames with a threshold number (N), and to send a warning signal when the number of discarded frames exceeds a threshold criterion.

* * *

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.